THE CROSSWALK
Threat Intelligence · Issue 01

TLP:CLEAR

THREAT INTELLIGENCE BRIEFING

ShinyHunters

History, structure, tradecraft, and what the world's most consequential data-theft brand means for higher-education SaaS.

PUBLISHED
May 12, 2026

AUDIENCE
CISO · Executive · Board

SERIES
Threat Intel · 01

PUBLICATION
thecrosswalk.news

Inside this briefing

A LONG READ IN NINE SECTIONS

> **A note on how to read this.** Section 1 is plain language and complete on its own. Sections 2 through 9 progressively increase in technical depth. A reader who stops at Section 1 walks away with the decision-grade picture; a reader who continues gets the engineering substrate behind those decisions.

01

SECTION ONE

Executive Summary

> A plain-language read for boards and CEOs. The bottom line, the business stakes, and the three decisions that matter most.

Bottom line up front

ShinyHunters is the single most consequential data-theft and extortion brand operating in the English-speaking cybercrime ecosystem as of mid-2026. Since 2020 they have been credibly linked to breaches affecting **well over a billion individual records** across more than 100 named victim organizations. Since August 2025 they have operated jointly with Scattered Spider and LAPSUS$ under a combined brand called **Scattered LAPSUS$ Hunters** (SLH).

They do not encrypt systems. They steal data, threaten to publish it, and ask to be paid not to. They have repeatedly demonstrated that **paying does not necessarily end the extortion** — most notably in the PowerSchool case, where individual K-12 school districts were re-extorted months after the parent vendor paid $2.85 million in bitcoin.

1B+
RECORDS LINKED TO SHINYHUNTERS-ATTRIBUTED BREACHES SINCE 2020

100+
NAMED VICTIM ORGANIZATIONS ACROSS ALL SECTORS

8,800
EDUCATIONAL INSTITUTIONS CLAIMED IN THE MAY 2026 CANVAS BREACH ALONE

Why this matters for a higher-education SaaS vendor

ShinyHunters has **explicitly and repeatedly chosen education-technology platforms as targets**. The PowerSchool breach (December 2024; ~62 million students and ~9.5 million teachers across roughly 6,505 districts) and the two-incident Instructure / Canvas campaign (a September 2025 Salesforce-based intrusion followed by an April–May 2026 Canvas breach the actor claimed affected 275 million users across ~8,809 institutions including Harvard, Stanford, MIT, Penn State, Duke, and others) show that the group understands the force multiplier of a multi-tenant edtech vendor.

One successful intrusion at the SaaS provider produces hundreds or thousands of downstream institutional victims simultaneously — each with their own legal notification obligations, parent or student notification obligations, regulatory exposure under FERPA, GLBA, and state breach laws, and reputational fallout.

⚠ THE "TOO SMALL OR TOO BORING" FALLACY

Both PowerSchool and Instructure were doing many things right. PowerSchool's CEO had spoken at a 2023 White House cybersecurity summit before the breach. Both were hit through identity-layer vectors that work against vendors of any size. A vendor in this position cannot reasonably assume it is too small or too boring to be a target. The asymmetry between data value and security maturity is what attracts the group, not the size of the logo.

The three things a CEO or board member needs to act on

1 · IDENTITY IS THE PERIMETER

ShinyHunters and SLH almost never exploit software vulnerabilities. They exploit help-desk verification, employee or contractor MFA, and OAuth tokens granted to legitimate third-party SaaS applications. The single most decisive control is enforced **phishing-resistant MFA** (FIDO2 / WebAuthn / hardware keys) for every employee, contractor, and privileged or break-glass account, plus a help-desk identity-proofing process that does not rely on knowledge-based answers and that requires out-of-band verification for any password or MFA reset.

2 · YOUR THIRD-PARTY SAAS STACK IS PART OF YOUR ATTACK SURFACE

The two biggest SaaS-vendor incidents of 2025 — the Salesloft Drift OAuth-token theft (700+ organizations including Cloudflare, Zscaler, Palo Alto Networks, Proofpoint, and Google) and the November 2025 Gainsight Salesforce-integration compromise — both used **stolen OAuth tokens, not stolen passwords**. Every connected SaaS application is a credential. Every connected SaaS application needs an owner, a review cadence, and a revocation procedure.

3 · PLAN FOR THE BREACH YOU CANNOT PREVENT

Treat a ShinyHunters-style intrusion as a "when, not if" scenario for any SaaS provider in higher education. The board-level decisions that matter most are pre-decided: **ransom payment policy, cyber-insurance triggers, customer-notification language, regulator-notification timing, and crisis-communications ownership**. The group's demonstrated pattern is to extort the vendor, then re-extort the vendor's customers individually with the same data, and to publicly defame organizations that do not pay through dedicated leak sites and Telegram channels.

What past victims actually paid

Victim	Posture	Outcome
AT&T (2024)	Paid ~$370K BTC through intermediary	Data still partially recirculated
PowerSchool (2024–25)	Paid $2.85M BTC	Districts re-extorted May 2025; ~100 lawsuits, multiple state AG CIDs, $14.1M restitution exposure
Coinbase (2026)	Refused $20M demand; offered $20M reward	Costly short-term, held up reputationally
Instructure (2026)	Ignored, patched silently → re-breached	Login pages defaced at ~330 institutions; Canvas taken offline during finals week; later reached "agreement"

The pattern is consistent: **the direct ransom is rarely the largest cost.** Litigation, regulatory enforcement, customer-contract liability, and the lasting trust erosion among institutional buyers are.

02

SECTION TWO

History and Timeline

> Six years, three major rebrands, multiple arrests, and an alliance with two other groups. The strategic arc of a brand that has outlived every attempt to dismantle it.

The arc, in one paragraph

ShinyHunters surfaced on dark-web forums in late 2019 / early 2020, named for the Pokémon-fandom practice of grinding for rare alternate-color creatures. They made their public debut in May 2020 with a burst of breaches across more than a dozen companies in roughly two weeks. They became **BreachForums** administrators. They drove the 2024 Snowflake supply-chain campaign. They executed the largest education-data breach in U.S. history (PowerSchool, December 2024). They built and ran the 2025 Salesforce vishing campaign. They merged with Scattered Spider and LAPSUS$ in August 2025. They breached Canvas during finals week 2026. They have absorbed multiple arrests — Raoult in 2022, Moucka and Binns in 2024, IntelBroker and four French nationals in 2025 — without operational disruption.

Major incidents and inflection points

May 2020

Public debut

Burst of breaches in ~2 weeks: Tokopedia (91M), Wishbone, Microsoft GitHub claim, Mathway (25M), Wattpad (270M), Home Chef, Minted, Chatbooks, Zoosk, and more.

2021

AT&T listing on RaidForums

70M AT&T wireless subscriber records listed for sale. AT&T did not publicly acknowledge the breach until 2024.

May 2022

First arrest: Sébastien Raoult

French national "Sezyo Kaizen" arrested in Morocco at U.S. request. Extradited January 2023; sentenced January 2024 to 3 years prison + $5,000,001 restitution. DOJ described him as "not a major player." Operations continued uninterrupted.

Apr–Jul 2024

Snowflake supply-chain campaign

UNC5537 (Mandiant tracking) logged into ~165 Snowflake customer instances using infostealer-harvested credentials. Victims: Ticketmaster (560M records), AT&T (110M call/text metadata; AT&T paid ~$370K BTC), Santander (30M), LendingTree, Advance Auto Parts, Neiman Marcus, Pure Storage. Snowflake itself was not breached.

Jun–Jul 2024

Authy / Twilio dump

33.4 million Authy phone numbers harvested via unauthenticated API enumeration.

Oct 2024

Moucka arrest

Connor Riley Moucka ("Waifu" / "Judische") arrested in Kitchener, Ontario for Snowflake-campaign offenses.

Dec 2024

PowerSchool breach

Matthew D. Lane, 19, used credentials stolen from a PowerSchool contractor. 106 days of dwell time. ~62M students + ~9.5M teachers across ~6,505 districts. PowerSchool paid $2.85M BTC. Districts were re-extorted starting May 2025.

Feb 2025

IntelBroker arrest

Kai West, 25, British national operating as "IntelBroker," arrested in France. SDNY indictment alleges $25M in losses.

Jun 2025

Salesforce vishing campaign disclosed

Google Threat Intel Group publicly attributes UNC6040 — Salesforce Data Loader OAuth abuse via voice phishing. Victims through 2025 include Google, Cisco, Adidas, Qantas (5.7M), Allianz Life (2.8M), Workday, Pandora, Chanel, LVMH (Louis Vuitton, Dior, Tiffany), Kering (Gucci, Balenciaga), Air France-KLM.

Jun 23, 2025

French BL2C arrests

Four early-twenties suspects arrested in Paris, Normandy, and La Réunion — operating as ShinyHunters, Hollow, Noct, Depressed. Brand kept operating regardless.

Aug 8, 2025

Scattered LAPSUS$ Hunters formed

Telegram channel launches combining the three brands. ShinyHunters publicly describes the division of labor: Scattered Spider does initial access, ShinyHunters does data theft/dumps, LAPSUS$ does extortion theatrics.

Aug 2025

Salesloft Drift OAuth theft

UNC6395 abuses Drift OAuth tokens stolen from Salesloft's GitHub repos earlier in 2025. 700+ Salesforce instances affected, including Cloudflare, Google, Palo Alto Networks, Zscaler, Proofpoint, PagerDuty, CyberArk.

Sep 12, 2025

FBI FLASH alert

IC3 publishes FLASH-20250912-001 on UNC6040 and UNC6395 with IOCs and recommended mitigations.

Sep 2025

Instructure incident #1

Instructure's Salesforce instance compromised via social engineering. Instructure states no Canvas product data accessed.

Oct 10, 2025

FBI/BL2C domain seizure

Clearnet ShinyHunters leak-site domain seized; replaced with seizure notice.

Nov 19, 2025

Gainsight + ShinySp1d3r

ShinyHunters discloses Gainsight Salesforce-integration abuse (~285 instances). Same day: ShinySp1d3r ransomware sample uploaded to VirusTotal, marking the brand's first move into encryption-based monetization.

May 2026

Instructure / Canvas — finals week

Free-For-Teacher account abuse → unauthorized Canvas access. ShinyHunters claims 3.65 TB / ~275M users / ~8,809 institutions. After Instructure publicly states "contained" without negotiating, group re-breaches May 7, defaces ~330 Canvas login pages, forces Canvas offline globally during finals week. Instructure confirms "agreement" reached on May 11.

▸ THE PATTERN THAT MATTERS

Every arrest cycle — Raoult (2024), Moucka and Binns (late 2024), West (February 2025), the four French BL2C arrests (June 2025), the alleged October 2025 "Shiny" arrest (unconfirmed), Stokes (April 2026) — has been followed by continued operations. The brand survives because operators are interchangeable and recruitment from the broader "Com" ecosystem is faster than prosecution.

03

SECTION THREE

Makeup, Structure, and Culture

> A federated cartel, not a corporation. Young Western operators, loose hierarchy, and an alliance that divides labor across three brands.

What ShinyHunters is — and is not

ShinyHunters is best understood not as a hierarchical criminal organization but as a **brand, a leadership cell, and a constellation of overlapping operators**. Google Threat Intelligence Group tracks the activity that wears the ShinyHunters label across multiple distinct intrusion clusters — UNC6040, UNC6240, UNC5537, UNC6395 (with caveats), UNC6661, UNC6671 — to keep technical attribution separate from branding.

The leadership persona "ShinyCorp" (also appearing as Shiny, sp1d3rhunters, and shinyc0rp across Telegram channels) is the publicly visible spine of the brand. Multiple researchers — DataBreaches.net, Obsidian Security, Truesec — recommend treating ShinyHunters and Scattered Spider as effectively a single coordinated entity rather than rigidly separate groups.

The Scattered LAPSUS$ Hunters alliance, visualized

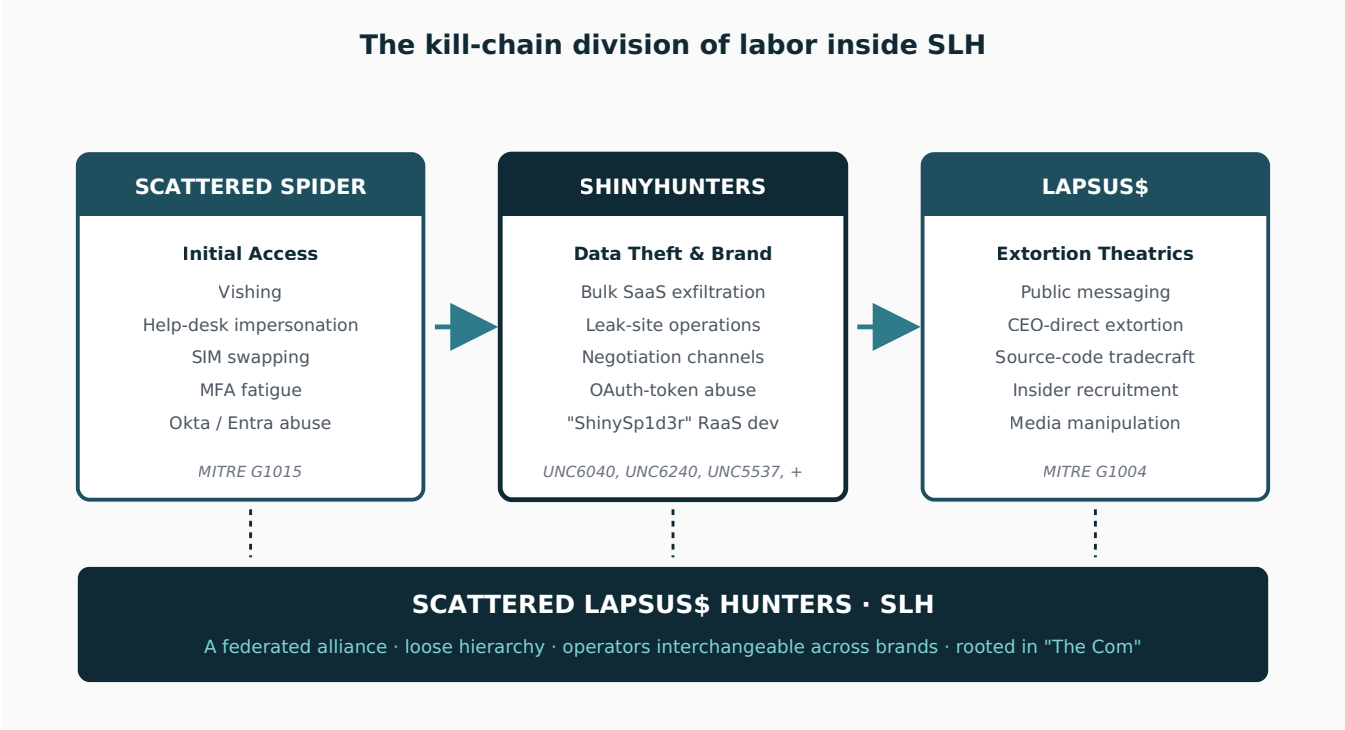

Figure 1 — Documented division of labor across the SLH alliance, per ShinyHunters' own Telegram statements and corroborating research from Mandiant/GTIG, Trustwave SpiderLabs, ReliaQuest, and EclecticIQ.

Membership and demographics

Public reporting identifies operators as primarily **young (late teens to mid-twenties), English-speaking, and based in the U.S., U.K., Canada, France, and elsewhere in Europe and Australia.** Confirmed arrestees illustrate the profile:

Handle	Name / Origin	Age	Arrest / Outcome
Sezyo Kaizen	Sébastien Raoult / French	22 at sentencing	Morocco 2022 → 3 yrs US prison Jan 2024
—	Matthew D. Lane / U.S. (MA)	19 at offense	4 yrs prison Oct 2025; $14.1M restitution
Waifu / Judische	Connor Riley Moucka / Canadian	25	Kitchener Oct 2024 (Snowflake)
IRDev	John Erin Binns / U.S.	24	Turkey May 2024
IntelBroker	Kai West / British	25	France Feb 2025
Shiny/Hollow/Noct/ Depressed	Four French nationals	early 20s	BL2C arrests Jun 23, 2025
Bouquet	Peter Stokes / Estonian-U.S.	19	Helsinki Apr 10, 2026

The pattern is overwhelmingly young, Western, technically self-taught, and frequently with roots in adjacent online subcultures — competitive gaming, Roblox cheating communities, SIM-swapping crews, and crypto-fraud networks. Lane, in his own post-conviction interviews, described starting with Roblox cheats at age 14, calling the path a "very toxic and edgy corner of the internet."

"The Com" — the recruitment substrate

Both Scattered Spider and ShinyHunters are routinely described by Mandiant, the FBI, and others as affiliated with **"The Com"** (short for "The Community"), a loosely connected, primarily English-speaking, predominantly minor and young-adult online network. Members coordinate on Telegram and Discord, share TTPs and infrastructure, and migrate between named brands.

Researcher Allison Nixon (Unit 221B) has characterized The Com as roughly **1,000 active participants in shifting partnerships** — "a huge spaghetti soup" — that has collectively breached organizations with more than **$1 trillion in combined market cap since 2022**. A notable demographic shift in 2024–2025 has been the rapid increase in teenage and young-adult women in The Com, particularly in vishing-caller roles where a neutral, polite female voice on a help-desk call lowers victim suspicion.

Motivations

- **Financial.** Primary. Ransom demands range from low-six figures to tens of millions. Beyond ransoms: data sales, credential resale, and (newly) RaaS affiliate fees.

- **Notoriety and clout.** Members openly engage with journalists at BleepingComputer, TechCrunch, and Wired. They taunt victims publicly, address open extortion letters to CEOs (a $20 million BTC demand was publicly addressed to Salesforce CEO Marc Benioff), and curate persona reputations.
- **Ideological / performative.** Limited but present. SLH has publicly threatened to deanonymize U.S. federal employees and to claim FBI-related data. The collective brands itself with hacktivist aesthetics despite an unambiguously financial motive.

Communication channels and operational tempo

- **Telegram** — primary live channel. At least 16 named iterations of the "scattered LAPSUS$ hunters" channel through late 2025 (Trustwave SpiderLabs count), repeatedly banned and re-spun.
- **BreachForums** — primary marketplace through 2024–2025. ShinyHunters relaunched BreachForums (v4) in June 2025 immediately after IntelBroker's arrest became public. Following the October 2025 FBI seizure, the alleged leader publicly warned that any reappearance should be treated as a law-enforcement honeypot. **DarkForums** has emerged as the most cited successor.
- **Tor leak sites** — `shinyhunte[.]rs`, `breachforums[.]hn`, and onion equivalents.
- **X (Twitter) and Discord** for amplification and recruitment.
- **Insider recruitment** — explicit Telegram posts since August 31, 2025 offering payment for Okta, Microsoft SSO, Citrix VPN, GitHub, or GitLab access.

04

SECTION FOUR

Tactics, Techniques, and Procedures

> Mapped to MITRE ATT&CK. They do not need zero-days. They need a phone, an OAuth flow, and a help-desk that resets MFA on demand.

The TTP picture in one sentence

ShinyHunters / SLH tradecraft is **unsophisticated by elite-APT standards** — no zero-days, no novel exploits, no advanced malware until the (still in development) ShinySp1d3r encryptor. What makes them dangerous is the combination of disciplined targeting, opportunistic credential harvesting, fluent social engineering, an open recruitment pipeline, and a public-extortion playbook calibrated to extract maximum settlement leverage from victims who cannot tolerate disclosure.

4.1 · Initial access

Vishing and help-desk social engineering

`T1566.004` `T1656` The dominant initial-access vector since late 2024. UNC6040 operators call English-speaking employees, impersonating internal IT support, often using a "closing an auto-generated ticket" pretext (per FBI FLASH-20250912-001). In the Salesforce Data Loader variant, the caller directs the employee to Salesforce's connected-app authorization page, provides an eight-digit code, and induces them to authorize the attacker's modified Data Loader build (observed branding: `My Ticket Portal`). The MGM Resorts 2023 breach — attributed to Scattered Spider — used the same playbook.

AI-assisted vishing

EclecticIQ assesses with high confidence that ShinyHunters has begun deploying **AI voice agents** to automate vishing at scale, tailoring responses in real time and producing realistic regional accents. Fortune's January 2026 reporting documented The Com using AI voice modification to mimic specific demographics.

Credential theft via infostealers

`T1555` `T1539` `T1078` UNC5537's mid-2024 Snowflake campaign was driven entirely by credentials harvested by commodity infostealer families — **VIDAR, RISEPRO, REDLINE, RACOON STEALER, LUMMA, METASTEALER** — purchased or aggregated from underground marketplaces. Mandiant's investigation found that some Snowflake credentials in active use had been originally stolen as far back as 2020. The threat actor did not deploy infostealers themselves; they purchased the logs. Infections were observed on non-Snowflake-owned endpoints, including third-party contractor systems used for personal activities (gaming, pirated downloads).

OAuth abuse and malicious connected-app consent

`T1528` `T1199` The single most distinctive ShinyHunters tradecraft of 2025. Two major variants:

- **Vishing-induced OAuth grant.** (UNC6040 / Salesforce Data Loader, throughout 2025.) Victim is socially engineered into authorizing the attacker's app.
- **Supply-chain OAuth token theft.** (UNC6395 / Salesloft Drift, August 2025; ShinyHunters / Gainsight, November 2025.) Attackers compromise a third-party vendor's GitHub, steal OAuth and refresh tokens

used by that vendor's Salesforce-connected application, and use the tokens to impersonate the legitimate app against every downstream customer. *No interaction with the customer is required.* The attack appears in logs as the trusted integration doing what it normally does.

4.2 · Persistence, escalation, lateral movement

- **Token theft and abuse for persistence** `T1550.001` `T1098.001` — Captured OAuth refresh tokens give persistent, MFA-bypassing access until revoked.
- **MFA bypass and modification** `T1556.006` — Push bombing / MFA fatigue and registration of attacker-controlled MFA tokens. SIM swap for SMS-based MFA interception remains common in Scattered Spider tradecraft.
- **Domain trust and federation abuse** `T1484.002` — Scattered Spider has been observed adding rogue federated identity providers and activating account linking in the victim's SSO tenant to elevate privileges.
- **SaaS-to-SaaS pivot** — Salesloft → Drift → Salesforce → Snowflake/AWS via harvested keys is the most distinctive 2025 escalation chain.

4.3 · Discovery, collection, exfiltration

- **Cloud / SaaS reconnaissance** `T1538` `T1526` — UNC6395 ran small, low-volume SOQL reconnaissance queries before bulk exports. UNC6040 made numerous small test queries before scaling once detection thresholds were established.
- **Bulk data harvesting** `T1213` `T1530` — Heavy focus on Salesforce Accounts, Contacts, Cases, Opportunities, and Users objects. Snowflake Bulk API exports against standard data tables.
- **Credential hunting in stolen data** `T1552` — UNC6395 explicitly hunted exported Salesforce data for AWS access keys (`AKIA` prefix), Snowflake tokens, VPN credentials, and passwords embedded in support cases — feeding the next attack cycle.
- **Anti-forensics in SaaS** `T1070` — UNC6395 deleted Salesforce query jobs after exfiltration.

4.4 · Tooling and infrastructure

Tool / Infrastructure	Use
Salesforce Data Loader	Abused as the data-export engine in UNC6040 operations. Sometimes renamed/rebranded as `My Ticket Portal`.
Python automation	UNC6395 used Python with `aiohttp` (user-agent `Python/3.11 aiohttp/3.13.1` documented by Mitiga) against Salesforce Bulk API. UNC6040 has shifted to custom Python scripts.
DBeaver + Snowflake Python Connector	UNC5537 used both to authenticate to Snowflake instances.
"FROSTBITE" / "rapeflake"	Mandiant-observed custom toolkit used by UNC5537 against Snowflake to automate enumeration and bulk export across multiple targets.
Mullvad / PIA / Tor exits	Primary egress obfuscation.
Cloud-resident infrastructure	Azure VMs, AWS infrastructure, ALEXHOST VPS (Moldova), MEGA for exfil storage.
Tox	Preferred negotiation channel.
Limewire	Sample-hosting platform for stolen-data proof posts in UNC6240 extortion.

4.5 · Extortion and monetization

Through 2024 and most of 2025, ShinyHunters did not deploy ransomware. The extortion model has been:

1. Quietly exfiltrate large volumes of data.
2. Wait days, weeks, or months to maximize victim panic and to establish that data is real and current.
3. Send extortion email referencing specific objects/tables stolen, naming the data set, specifying a BTC address and amount. Typical demand: **72-hour deadline**.
4. Escalate to publication on a public DLS if unpaid.
5. Re-extort downstream customers / individual end-users using the same stolen data.

⚠ **SHINYSP1D3R — THE PIVOT TO ENCRYPTION**

The November 2025 emergence of **ShinySp1d3r** marks a strategic move into encryption-based monetization. Coveware analysis of the in-development Windows encryptor describes an unusually feature-rich build (not derived from leaked LockBit / Babuk code): ChaCha20 with RSA-2048 key wrap, `EtwEventWrite` hooking to suppress Windows event logging, Shadow Volume Copy deletion, free-disk-space overwrite, process termination for held file handles, and propagation via WMI, services, and GPO startup scripts. Linux and ESXi builds, plus a "lightning version" written in pure assembly, are stated as forthcoming. **Operational deployment in mid-to-late 2026 is the working assumption.**

4.6 · Distinctive operational signatures

- Extortion emails branded "We are ShinyHunters" using first-person plural — even after individual arrests.
- 72-hour ransom deadline as a documented norm in UNC6240 extortion emails.
- Common Tox account for negotiations across UNC6040 / UNC6240 / UNC6661 clusters.
- De-listing victims from the DLS shortly after the victim opens contact — in the May 2026 Instructure removal, this was the public tell that negotiations had begun.
- Public address-by-name of CEOs (Benioff at Salesforce; Coinbase leadership).
- Use of Limewire as the preferred proof-sample host.

05

SECTION FIVE

Why Edtech and Higher Ed

> Multi-tenant SaaS as a force multiplier. Two case studies — PowerSchool and Instructure — that show the full life cycle from intrusion through re-extortion.

Why this sector specifically

ShinyHunters' targeting selection is rationally driven by three converging factors that higher-education SaaS vendors exhibit at an unusually high level.

▸ **RICH, REGULATED, AND DURABLE PII**

Higher-education systems hold full names, dates of birth, government-issued identifiers, Social Security numbers, passport and visa data for international students, immigration status, financial-aid award data, family financial information from the FAFSA process, medical records (disability accommodations, counseling services), academic transcripts, and private student-faculty communications. **Unlike credit-card numbers, which can be reissued, much of this data is permanent.** Stolen student SSNs from minors have particular black-market value precisely because the victims will not check their credit for years.

▸ **MULTI-TENANT SAAS = FORCE MULTIPLIER**

A single vendor breach affects every customer institution simultaneously. PowerSchool: one breach, ~6,505 districts. Snowflake: ~165 customer instances. Salesloft Drift: 700+ organizations. Instructure Canvas: ~8,809 institutions claimed. The economic ratio between attacker effort and reachable victim records is **uniquely favorable in vendor-of-vendors SaaS**.

▸ **CONSTRAINED CUSTOMER-SIDE BUDGETS + REPUTATIONAL SENSITIVITY**

Most higher-education institutions operate with security headcount and tooling significantly below the level of a Fortune 500 enterprise. They are also extraordinarily sensitive to public disclosure. **This combination produces an asymmetric pressure-to-pay relationship**: weaker defenses, higher willingness to negotiate to avoid disclosure.

Cascading regulatory exposure

A single breach at a higher-ed SaaS vendor can trigger:

Regime	Trigger
FERPA (20 U.S.C. § 1232g)	Department of Education's Student Privacy Policy Office; loss of FERPA-compliant standing affects federal funding. PowerSchool received a FERPA review.
GLBA Safeguards Rule	Financial-aid data; FTC's amended rule imposes a 30-day breach notification for incidents involving 500+ consumers.
State breach laws	All 50 U.S. states + Canadian provinces. NY Education Law 2-d requires 10-day notification to state Chief Privacy Officer.
UK Data Protection Act 2018 / UK GDPR	72-hour ICO notification for U.K. customer institutions.
Kuwait CITRA Data Privacy Regulation (2021)	Breach notification + regulator authority for Kuwaiti customers.
Qatar PDPPL (Law No. 13 of 2016)	Breach obligations for Qatari customers.
State AG Civil Investigative Demands	North Carolina AG Jeff Jackson's June 2025 CID to PowerSchool is the template.
Civil litigation	PowerSchool has faced 100+ lawsuits including class actions alleging negligence, FERPA-related claims, and CCPA violations.

Case study · PowerSchool

⚠ THE SINGLE MOST INSTRUCTIVE CASE STUDY FOR ANY HIGHER-ED SAAS VENDOR

PowerSchool served approximately **75% of the U.S. K-12 market**, operated in 90+ countries, and was used by 18,000+ schools across North America. It had been acquired by KKR and Dragoneer for $4.8 billion one month before the breach. The CEO had spoken at the White House's 2023 cybersecurity summit. The company was publicly positioned as a security leader.

Attack path

Matthew D. Lane, a 19-year-old freshman at Assumption University in Worcester, Massachusetts, obtained credentials belonging to a **PowerSchool support contractor** — credentials he reportedly "found online," consistent with the broader infostealer-log marketplace pattern. The credentials provided access to PowerSchool's PowerSource customer-support portal, which **lacked MFA enforcement**. First access: September 2024.

Dwell time

Approximately **106 days** passed between initial access and the December 28, 2024 extortion message. During this period Lane moved from "1 school district's data" to "1000s of districts' data." PowerSchool's internal detection capability did not surface the intrusion. The company became aware only because Lane contacted them and demanded payment.

Data scope

62M
STUDENTS ACROSS ~6,505 DISTRICTS

9.5M
TEACHERS ACROSS THE U.S. AND CANADA

106
DAYS OF UNDETECTED DWELL TIME

Per court filings, access included names, email addresses, phone numbers, Social Security numbers (for fewer than 25% of registered students per PowerSchool — still tens of millions of individuals), dates of birth, medical information, residential addresses, parent/guardian information, passwords, Individualized Education Plans (IEPs), and disciplinary records.

The ransom and the re-extortion

PowerSchool paid approximately **$2.85 million in bitcoin** and received a video purporting to show the data deleted. Beginning in May 2025, **individual school districts** — including the Toronto District School Board — began receiving extortion messages with samples of the same stolen data, demanding new ransom payments. PowerSchool's statement: this was not a new breach. From the victims' perspective: same data, different leverage point.

Legal and regulatory fallout

- Lane pleaded guilty June 2025 to four federal charges; sentenced October 15, 2025 to **4 years prison + $14.1M restitution + $25K fine**.
- U.S. Department of Education FERPA-compliance review opened.
- North Carolina AG public CID June 2025 (~4M North Carolinians affected). California and multiple other states opened parallel investigations.
- 100+ district lawsuits + class actions. Alleged breach-related compensation fund of ~$28M.
- Multiple states transitioned districts from PowerSchool to alternative SIS platforms (Infinite Campus). **Material contract-loss risk for any higher-ed SaaS vendor in a similar position.**

▸ THE TAKEAWAY

PowerSchool's published security posture was, on paper, strong. **The vulnerability was a single set of unrotated contractor credentials and a customer-support portal without MFA.** The 106-day dwell time reflects a detection-engineering gap that is endemic in mid-size SaaS: behavioral monitoring of normal employee/contractor access patterns to admin portals is rarely instrumented. Every credential is a potential breach. Every contractor is a potential entry point.

Case study · Instructure / Canvas

The Instructure pattern is even more directly relevant to higher-ed SaaS because Canvas is the dominant LMS in higher education in North America (~41% market share per the company), used by 30+ million active users at 8,000+ institutions. The two-incident sequence shows the full ShinyHunters life cycle.

Incident 1 (September 2025)

Social-engineering attack against Instructure's Salesforce instance, part of the broader UNC6040 vishing wave. Per Instructure, no Canvas product data was accessed. ShinyHunters publicly claimed the incident before Instructure had completed its investigation — consistent with their pressure playbook. Trade-press coverage only.

Incident 2 (April–May 2026)

Approximately eight months later, attackers exploited a vulnerability in Instructure's **Free-For-Teacher account program** — a low-friction onboarding flow that allowed educators to create Canvas tenants without institutional verification, sharing underlying infrastructure with paid institutional tenants. The architecture relied on logical rather than physical isolation; weak verification allowed attackers to gain unauthorized access to production Canvas data.

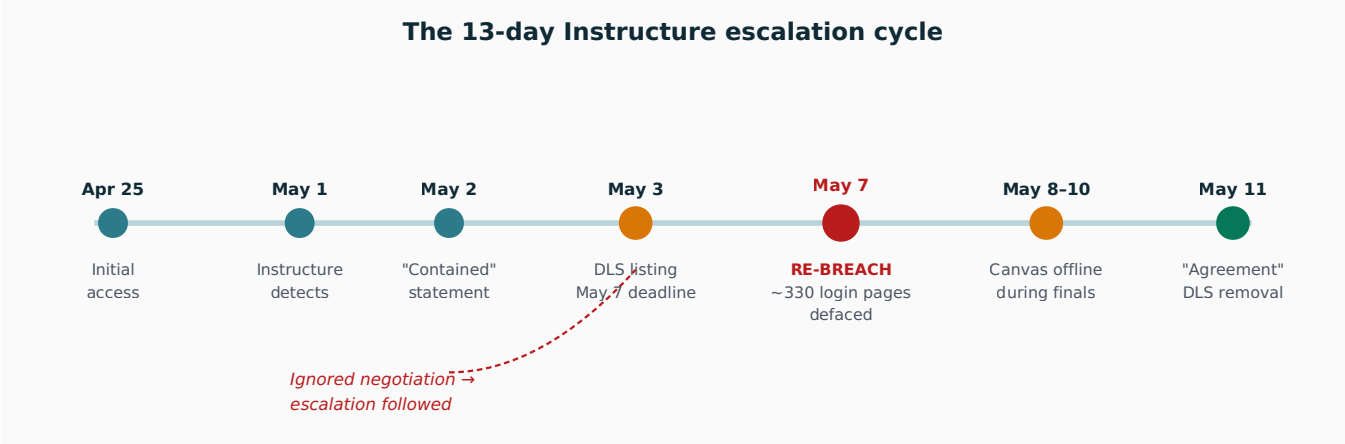

Figure 2 — Timeline of the May 2026 Instructure / Canvas incident. The re-breach on May 7 followed Instructure's May 2 "contained" statement; defacement of ~330 Canvas login pages forced the platform offline during finals week.

ShinyHunters claimed **3.65 TB** of data covering ~275 million users and ~8,809 institutions. Universities affected included Duke, the University of Pennsylvania, UC Irvine, Georgetown, East Carolina University, Pitt County Schools, and reportedly Harvard, Stanford, MIT, Columbia, Princeton, Yale, and Penn State. Confirmed data: names, email addresses (largely .edu accounts), student ID numbers, and Canvas inbox messages. Instructure stated no evidence of password, DOB, government ID, or financial data compromise.

> ▸ **THREE LESSONS FROM INSTRUCTURE**
>
> **First**, the second incident exploited a tenant-isolation weakness in a free-tier onboarding flow that was almost certainly not on the company's top-priority risk register before the breach. **Second**, the re-breach following a public "contained" statement and silent patching demonstrates that ignoring negotiation is itself a strategic choice with consequences — the group escalated to login-page defacement specifically as retaliation. **Third**, the finals-week timing maximized institutional pressure and made the outage front-page news at major universities, dramatically amplifying reputational damage.

The Snowflake campaign's implications for higher-ed SaaS

Even though Snowflake itself is not an edtech vendor, the 2024 Snowflake campaign is the most important precedent for any higher-ed SaaS vendor's posture on third-party data warehouses and analytics platforms. The campaign succeeded because of three identifiable failures, every one of which is replicable at any SaaS company:

1. Customer Snowflake accounts **lacked MFA**. (Snowflake's shared-responsibility model placed MFA on the customer; mandatory MFA was only announced June 10, 2024 — after the breaches.)
2. Credentials in infostealer logs had not been rotated. **Some were years old.**
3. Network allow-lists were not configured to restrict access to trusted locations.

For a higher-ed SaaS vendor, the lesson generalizes: **any time you ingest credentials from a customer, or push data to a third-party analytics / warehouse / integration partner, those credentials and those data flows are part of your breach exposure**. The 2026 Rockstar Games incident, in which ShinyHunters claimed access to Rockstar's Snowflake instance via the Anodot analytics connector, is the worked example.

06

SECTION SIX

Threat Model

> Five generic attack paths against a higher-ed multi-tenant SaaS vendor, ranked by probability. Scenarios drawn from documented ShinyHunters tradecraft.

How they would actually come at you

This section presents a generic threat model for a higher-education multi-tenant SaaS vendor. It makes no assumptions about specific architecture, beyond the publicly visible facts that the company serves universities across multiple jurisdictions. Attack paths are in descending order of probability, anchored to ShinyHunters' demonstrated targeting and tradecraft.

ATTACK PATH 01

Help-desk social engineering for credential / MFA reset

HIGHEST PROBABILITY

TECHNIQUE

Operator places a phone call to a vendor employee, contractor, or outsourced help-desk agent, impersonating a senior employee, IT, or a third-party vendor representative. Pretext is often urgent. Some variants use AI-generated voice modification. Operator pushes for password reset, MFA token reset, or registration of a new authenticator device under their control.

SCENARIO

A help-desk technician on the night shift receives a call from someone claiming to be a senior engineer who is at an airport, has lost their phone, and needs their MFA reset urgently before a deployment window closes. The caller has the employee's full name, title, manager name, and recent project names — gleaned from LinkedIn and the company website. Knowledge-based verification questions are answered confidently. The technician resets the MFA. Within an hour the attacker has authenticated to the employee's email, SSO console, and SaaS admin tooling. Within a day, customer-data export tooling has been used. Within a week, the activity surfaces as bulk database query patterns.

WHY THIS IS THE HIGHEST-PROBABILITY PATH

It is the single most-used initial-access vector in all 2025 SLH operations. It requires no software vulnerability. It defeats traditional MFA. Outsourced help desks (common at higher-ed SaaS vendors) are explicitly identified by CISA AA23-320A and the FBI FLASH as Scattered Spider's preferred attack surface.

CONTROLS

- Phishing-resistant MFA (FIDO2 / WebAuthn) for **all** employees and contractors — NIST 800-53 IA-2(1)(2); CSF PR.AA-01; SOC 2 CC6.1
- Help-desk identity-proofing standard: two independent verification methods, at least one out-of-band and resistant to voice impersonation. Knowledge-based questions explicitly disallowed. NIST 800-53 IA-12; CSF PR.AA-02
- Cooling-off delay (15–30 min for general, 60+ for privileged) with parallel SOC notification
- Privileged-account resets routed to a "high-risk queue" — never tier-1
- Quarterly tabletops specifically modeled on the UNC6040 / Scattered Spider playbook
- For outsourced help desks: contractual identity-proofing, audit rights, joint tabletops, segmented access

ATTACK PATH 02

Infostealer credential harvesting → SaaS console access

HIGH PROBABILITY

TECHNIQUE

Commodity infostealer malware (LUMMA, REDLINE, RACOON STEALER, VIDAR, METASTEALER, RISEPRO) infects an employee or contractor endpoint, often via a malicious advertisement, cracked-software download, or browser extension. The stealer harvests saved browser passwords, session cookies, and authentication tokens. Logs are sold or published. Attackers test the credentials against SaaS admin portals.

SCENARIO

A long-tenured contractor's personal laptop, on which they have at some point checked their work Gmail or signed into the company VPN portal in a browser, is infected via a "free Adobe Premiere crack" download. Browser-saved credentials for the company SSO and a Snowflake or AWS console are exfiltrated. Months later (the Snowflake campaign demonstrated viable use of credentials up to four years old), a ShinyHunters operator buys the log, tries the SSO credential against the vendor's Okta portal, finds MFA disabled or weak, and gains access.

WHY THIS MATTERS

This is exactly the Snowflake campaign pattern. **The credentials don't need to be stolen from your network.** They can be stolen from any device a user used to authenticate, including unmanaged personal devices and contractor BYOD.

CONTROLS

- Phishing-resistant MFA enforced on **every** console — including service accounts, break-glass, and legacy auth paths
- Disable legacy authentication and password-only sign-in everywhere
- Network allow-lists / conditional access on admin consoles — NIST 800-53 AC-3(7), SC-7
- Continuous credential-exposure monitoring (Flare, SpyCloud, Recorded Future, Have I Been Pwned for Domains) — NIST 800-53 IR-6; CSF DE.CM-03
- Mandatory quarterly rotation + automatic rotation on infostealer hits
- Contractor endpoint requirements: managed device or MDM enrollment; no production access from unmanaged BYOD

ATTACK PATH 03

OAuth / connected-app abuse against integrated SaaS

HIGH PROBABILITY

TECHNIQUE

Either (a) *operator-induced consent*: an employee with administrative rights is socially engineered into authorizing a malicious connected app to the company's Salesforce / Workday / Microsoft 365 / Google Workspace; or (b) *supply-chain OAuth token theft*: a legitimate third-party SaaS vendor is compromised, and the OAuth/refresh tokens issued to its app are stolen and replayed against every customer that had the integration enabled.

SCENARIO

A marketing-ops manager who handles customer-onboarding tooling in Salesforce is socially engineered via a vishing call from "IT support" into authorizing a "ticket triage helper" app at the Salesforce connected-app authorization page. Eight-digit code, OAuth grant, done. The "helper app" has API access and exports the entire Salesforce contacts, accounts, and opportunities database over the next 48 hours. Detection comes from a sharp-eyed SOC analyst noticing an unfamiliar app in the connected-apps inventory two weeks later — or it doesn't come at all until an extortion email arrives.

WHY THIS MATTERS

This is the dominant 2025 ShinyHunters vector. **It is invisible to traditional perimeter defenses, defeats MFA, and is fundamentally a governance problem masquerading as a technical one.**

CONTROLS

- **OAuth app governance program.** Inventory every connected app. Approve via allow-list. Disable user-consent for new third-party apps; admin consent only — NIST 800-53 CA-3, CM-7; SOC 2 CC6.6
- Token lifetime restrictions and forced refresh-token rotation; revoke any OAuth refresh token unused for a defined period
- Quarterly review of every active integration, scope, and owning business unit
- Detection for new OAuth app authorizations as an alert; SOAR for automatic revocation pending review
- SaaS-to-SaaS posture management (Obsidian, AppOmni, Reco, Valence, DoControl, Push Security)
- Hunt for the specific IOCs published in FBI FLASH-20250912-001 and Mandiant's UNC6395 advisory

ATTACK PATH 04

Downstream university customer used to pivot into vendor

MEDIUM PROBABILITY

TECHNIQUE

ShinyHunters or an affiliate breaches a university customer (via vishing, infostealer, or a separate path). The customer's IT staff have legitimate credentials to the vendor's customer admin portal. The attacker uses those credentials to access the vendor's portal. From there: customer-data access, support-ticket access, and in some cases, lateral movement into vendor-side admin tooling if customer admins have unduly broad access.

SCENARIO

A help-desk technician at a mid-sized public university customer has their account compromised by Scattered Spider in a vishing call. The attacker discovers the university's admin credentials for the vendor's customer-tenant administration console. The attacker logs in, exports the institution's data, and then — discovering that the support portal allows cross-tenant search by support staff — pivots laterally to attempt access to other customers.

WHY THIS MATTERS

Higher-education customers are, on average, far less secure than higher-ed SaaS vendors. **The vendor inherits the attack surface of every customer's IT support team.**

CONTROLS

- Strict tenant isolation in customer admin portal; cross-tenant operations require explicit elevated authorization, heavy logging, SOC alerts — NIST 800-53 AC-4, SC-7
- Customer-side MFA enforcement: if a customer has not enabled MFA on their admin accounts, deny access or surface a compliance flag
- Step-up authentication for any bulk data export or administrative action from a customer account
- Behavioral anomaly detection on customer admin sessions (geographic shifts, off-hours bulk operations)
- Customer security guidance and contractual security baseline (also a marketing differentiator in 2026)

ATTACK PATH 05

Third-party vendor supply-chain compromise

MEDIUM PROBABILITY

TECHNIQUE

A SaaS vendor's own SaaS vendors (CRM, marketing automation, ticketing, data warehouse, observability, analytics) are compromised. OAuth tokens, API keys, or credentials issued by the higher-ed SaaS vendor to those third parties are then used to access the vendor's environment. The Salesloft Drift / Gainsight pattern, applied recursively.

SCENARIO

The higher-ed SaaS vendor uses a sales-engagement tool, a customer-success platform, and a BI tool, each integrated with their Salesforce or HubSpot. One of those vendors is breached. The attackers don't need to touch the higher-ed SaaS vendor's network at all — **the integration tokens give them direct API access** to read accounts, contacts, opportunities, support cases, and possibly call recordings or chat transcripts.

CONTROLS

- Maintained inventory of every SaaS-to-SaaS integration with token expiration, scope, and risk classification — NIST 800-53 CA-3, SR-3
- Least-privilege scoping of integration permissions; reject any vendor that demands write access it doesn't need
- Token rotation cadence; alerting on token use outside known integration IP ranges
- Continuous threat-intel monitoring for every in-use SaaS vendor (do you know within 24 hours when one of your SaaS vendors discloses a breach?)
- Contractual security baseline: SOC 2 Type II, breach notification SLA, MFA enforcement, OAuth scope documentation
- Emergency revocation runbook: immediate token revocation across all integrations with a vendor that has disclosed a breach

07

SECTION SEVEN

Defensive Recommendations

> Eight control families, mapped to NIST 800-53 Rev. 5, NIST CSF 2.0, and SOC 2. Identity is the perimeter — spend as if it were.

The control program in eight families

7.1 · Identity and authentication

- **Phishing-resistant MFA for everyone, no exceptions.** FIDO2 / WebAuthn / hardware-key-backed authentication for every employee, contractor, vendor, service account holder, break-glass account, and privileged-access account. **Push notifications, SMS OTP, and TOTP-only schemes are insufficient.** CISA's "Implementing Phishing-Resistant MFA" is the operational reference.
  NIST 800-53: IA-2(1), IA-2(2), IA-2(11), IA-2(12) · CSF: PR.AA-01, PR.AA-03 · SOC 2: CC6.1, CC6.6
- **Conditional access** by device compliance, network location, risk score, and authentication context — NIST 800-53 AC-2(12), AC-3(7); CSF PR.AA-05
- **Disable legacy authentication and password-only sign-in**, including for service accounts, automation accounts, and SaaS-local accounts that bypass corporate SSO
- **Token-lifetime restrictions**: aggressively short access-token lifetimes for SaaS admin consoles; force re-authentication for sensitive operations
- **Refresh-token rotation** enforced on every issuance; immediate revocation on credential rotation or device de-enrollment
- **No SMS for MFA, period.** SIM swapping is in the Scattered Spider documented toolkit.

7.2 · Help-desk identity proofing

- **Documented standard requiring two independent verification methods**, of which at least one must be out-of-band and resistant to voice / video impersonation — manager-attested live video call, authenticated corporate portal session with step-up, or in-person verification
  NIST 800-53: IA-12 · CSF: PR.AA-02
- Knowledge-based questions explicitly disallowed for sensitive operations
- Cooling-off delay between reset request and credential change
- Privileged-account and admin-tier resets routed to a dedicated trained "high-risk" queue; tier-1 cannot approve
- Vendor-run help-desk contracts include identity-proofing requirements, audit rights, MFA enforcement, logging retention, incident notification SLA, and joint tabletop participation

7.3 · Privileged access management and least privilege

- PAM tooling for every shared, admin, or break-glass credential; **just-in-time access elevation** rather than standing admin rights
  NIST 800-53: AC-6, AC-6(2), AC-6(5) · CSF: PR.AA-04, PR.AA-05 · SOC 2: CC6.2, CC6.3

- Least-privilege OAuth scopes on every connected app and service-to-service integration; the "API Enabled" Salesforce permission and analogues in other platforms should be tightly restricted
- Quarterly access reviews documenting who has admin / service / break-glass access to every business-critical SaaS and admin console

7.4 · OAuth and third-party SaaS governance

- **Inventory** every OAuth-connected app in every business-critical SaaS (Salesforce, Workday, Microsoft 365, Google Workspace, Slack, Snowflake, ServiceNow, CRM, BI, customer success, marketing automation)
  NIST 800-53: CM-8, CA-3 · CSF: ID.AM-02, ID.AM-04 · SOC 2: CC3.2
- **Admin-consent-only** for new third-party app authorizations; end-user consent disabled
- **Allow-list** of approved apps; everything else denied at the platform level
- Periodic review of every connected app's scope, business owner, and last-used timestamp; revoke dormant tokens
- **SaaS Security Posture Management (SSPM)** tooling for cross-SaaS visibility

7.5 · Logging, detection, and monitoring

- **Centralized SIEM** ingestion of authentication, admin, and API logs from every business-critical SaaS
  NIST 800-53: AU-2, AU-6, AU-12 · CSF: DE.CM-01, DE.AE-01 · SOC 2: CC7.2
- SaaS-specific detection use cases (full list in Section 8): new OAuth app authorization, bulk data export above threshold, Bulk API / Data Loader from non-typical IPs, login from Mullvad / Tor, FBI FLASH IOC user-agents, SOQL queries above baseline, query-job deletion
- Behavioral baselines for every privileged user (typical login hours, locations, API patterns) with UEBA-style anomaly detection
- Customer-portal anomaly detection: bulk operations from a customer tenant outside that customer's normal hours or volume
- **Log retention: minimum 12 months for SaaS audit logs, 24 months for authentication logs.** Most SaaS default retention is shorter; pull logs into your SIEM.

7.6 · Endpoint and credential hygiene

- EDR / XDR on every employee endpoint, with managed detection-and-response coverage
  NIST 800-53: SI-3, SI-4 · CSF: DE.CM-01, PR.IP-12 · SOC 2: CC7.1
- No personal-device access to production admin tooling
- **Infostealer monitoring service** configured for company domains and key employee identifiers — CSF DE.CM-03; NIST 800-53 IR-6

- Automatic credential rotation policy triggered by infostealer-log hits
- Disable browser password saving for production credentials; require enterprise password manager

7.7 · Incident response and resilience

- **Documented IR playbook specifically for a ShinyHunters-style intrusion**: pre-decided ransom-payment policy, board-level escalation triggers, regulator-notification timing, customer-notification language, legal counsel and forensic IR firm retainers

  NIST 800-53: IR-1 through IR-8 · CSF: RS.MA-01, RS.RP-01 · SOC 2: CC7.3, CC7.4, CC7.5
- Quarterly tabletop exercises modeled specifically on UNC6040, UNC6395, and Scattered Spider attack chains; include legal, comms, executive leadership, customer-success
- Customer notification readiness: pre-drafted templates, customer-by-customer notification workflow, decision-rights matrix
- Cyber insurance with explicit coverage for vendor-of-vendors scenarios, ransom payment, regulatory fines, customer-contract liability, IR retainers
- Backup and recovery for SaaS data with offline / immutable copies tested annually — directly applicable now that ShinySp1d3r is in development

7.8 · Customer-facing transparency and communications

- Public-facing security page describing controls, certifications, breach-notification SLA, and incident-history transparency
- Pre-negotiated SLA for breach notification to customers (typically 72 hours; faster than statutory minimums is a market differentiator)
- Breach-communication tone-of-voice document. The contrast between PowerSchool's silent-payment-then-public-exposure trajectory and Coinbase's public-refusal-plus-bounty trajectory illustrates how dramatically posture choices affect long-term reputation.

Authoritative advisories to track

Advisory	Source	Coverage
Joint CSA AA23-320A	CISA / FBI / RCMP / ASD ACSC / NCSC-UK	Scattered Spider TTPs with MITRE ATT&CK mapping (v17); July 2025 update
FLASH-20250912-001	FBI IC3	UNC6040 / UNC6395 Salesforce data theft and extortion; IOCs + mitigations
UNCxxxx series	Google Threat Intel Group / Mandiant	UNC5537 (Snowflake), UNC6040 (vishing), UNC6395 (Salesloft Drift), UNC6661 / UNC6671 (Jan 2026 expansion)
Implementing Phishing-Resistant MFA	CISA	Operational reference for FIDO2 deployment

08

SECTION EIGHT

Indicators and Detection

> Behavioral indicators, detection engineering priorities, and IOCs from primary public sources. Detection that watches authentication and OAuth, not perimeter.

Behavioral indicators that warrant investigation

The following patterns, derived from the documented UNC6040, UNC6240, UNC6395, UNC6661, UNC6671, and UNC5537 activity, should generate detection content in the SIEM and trigger SOC triage when observed.

Authentication and identity layer

- Successful authentication to an admin console or SaaS platform from a Mullvad VPN, Private Internet Access, NordVPN, or Tor exit-node IP range
- Authentication from a country, ASN, or time-of-day inconsistent with the user's baseline
- New MFA device registration for a privileged account within 24 hours of a help-desk ticket touching that account
- An MFA reset performed by tier-1 help desk on a privileged or executive account
- Multiple consecutive MFA challenges followed by acceptance — push bombing / MFA fatigue pattern
- A help-desk ticket closed unusually quickly that involved an MFA reset for a privileged account
- Account login from a fresh user-agent that doesn't match the user's normal browser fingerprint

SaaS application layer

- New OAuth connected app authorized to Salesforce / Microsoft 365 / Google Workspace / Workday / Snowflake / ServiceNow
- OAuth app named generically (`My Ticket Portal` , `Data Helper` , `Sync Tool` , `Integration Bridge`) with broad scopes
- API token used from an IP range that has never been associated with the legitimate vendor
- Salesforce Data Loader usage from an IP not on the corporate allow-list
- Bulk API export jobs from Salesforce / Workday / ServiceNow / Snowflake above per-user baseline
- SOQL queries against `User` , `Account` , `Contact` , `Case` , or `Opportunity` exceeding per-user baselines, especially with suspicious `LIMIT` values
- **Salesforce Bulk API query job deletion shortly after completion** — UNC6395 anti-forensics
- Salesforce login as a connected app shortly after that app was authorized — UNC6040 vishing-induced consent
- **OAuth refresh token used for the first time after a long period of dormancy** — Salesloft Drift / Gainsight token-replay pattern

Network, infrastructure, and email

- DNS lookups or outbound traffic to `shinyhunte[.]rs`, `breachforums[.]hn`
- Outbound traffic to MEGA, ALEXHOST VPS ranges (Moldova)
- User-agent strings consistent with FBI FLASH-20250912-001 IOCs
- The specific `Python/3.11 aiohttp/3.13.1` user-agent or close variants on Salesforce-like API access
- Inbound email from `shinycorp@tutanota[.]com`, `shinygroup@onionmail[.]com`
- Email referencing specific data inventories, 72-hour deadlines, BTC addresses, or Tox handles
- Internal-impersonation phishing referencing IT support, ticket numbers, or specific internal application names

Detection engineering priorities

#	Priority
1	**OAuth-grant detection** in Salesforce, Microsoft 365, Google Workspace, Workday, ServiceNow, Snowflake
2	**Bulk SaaS data export anomaly detection** keyed off historical user/role baselines
3	**Help-desk reset audit pipeline** correlating reset tickets with SIEM authentication events to flag mismatches
4	**Identity-provider session anomalies** (Okta / Entra ID): impossible-travel, unusual app launches, MFA-method changes, new device registrations
5	**Service-account / API-token abuse**: tokens used from new IPs, after dormancy, or for operations outside the documented integration's purpose
6	**External-mention monitoring** of company name on Telegram channels, DLS leak sites, paste sites, and BreachForums-successor venues (DarkForums)

Indicators of compromise — authoritative sources

- **FBI FLASH-20250912-001** (`ic3.gov/CSA/2025/250912.pdf`) — user-agent strings, IP addresses, Salesforce OAuth authorization URLs used by UNC6040 and UNC6395
- **Google Threat Intelligence Group / Mandiant** blog posts on UNC5537, UNC6040, UNC6395, UNC6661, UNC6671 — each contains corresponding technical indicators
- **CISA AA23-320A** (Scattered Spider) — comprehensive legitimate-tool list (AnyDesk, ScreenConnect, Splashtop, Pulseway, TeamViewer, Tactical RMM, and others repurposed for access)
- **ShinySp1d3r in-development Windows encryptor SHA256**: `3bf53cddf7eb98d9cb94f9aa9f36c211a464e2c1b278f091d6026003050281de`. As a debug build, hash-based

detection alone is insufficient; behavioral detection on `EtwEventWrite` hooking, Shadow Volume Copy deletion, and ChaCha20 / RSA-2048 file-header structures is recommended.

Threat-intelligence feeds worth subscribing to

- Google Threat Intelligence Group / Mandiant
- Microsoft Threat Intelligence (Octo Tempest / Storm)
- CISA cybersecurity advisories
- FBI IC3 FLASH alerts
- Sophos Counter Threat Unit
- Palo Alto Unit 42
- CrowdStrike Falcon Adversary Operations
- Recorded Future
- Trustwave SpiderLabs
- EclecticIQ
- ReliaQuest
- SOCRadar, Flare
- REN-ISAC (R&E sharing community)
- EDUCAUSE security community

MITRE ATT&CK group references

Group	MITRE ID	Aliases
ShinyHunters	No formal ID as of report date	Bling Libra (Unit 42); closest formal ref is Mandiant's UNCxxxx tracking series
Scattered Spider	**G1015**	Roasted 0ktapus, Octo Tempest, Storm-0875, UNC3944
LAPSUS$	**G1004**	Strawberry Tempest, DEV-0537

09

SECTION NINE

Strategic Outlook

> High-confidence forecasts and uncertain ones. The "when, not if" framing — and why pre-decided posture matters more than any control.

What to expect through 2026

The trajectory across 2024–2026 supports a small number of high-confidence forecasts and a small number of plausible-but-uncertain ones. They are presented separately.

High confidence

▸ **SHINYHUNTERS / SLH WILL CONTINUE OPERATING DESPITE FURTHER ARRESTS**

Every prior arrest cycle has been followed by continued operations. The brand survives because operators are interchangeable and recruitment from The Com is faster than prosecution.

▸ **VISHING AND OAUTH ABUSE WILL REMAIN THE DOMINANT INITIAL-ACCESS VECTORS**

They work, defeat traditional MFA, and require no zero-days. Defenders' best wins of 2025 (Salesforce / Salesloft MFA hardening, mandatory MFA at Snowflake) raise the cost but do not eliminate the technique. AI-assisted vishing will continue to scale, lowering the operator skill threshold.

▸ **SAAS-TO-SAAS SUPPLY-CHAIN ATTACKS WILL INCREASE**

The Salesloft Drift and Gainsight playbooks proved the model: compromise a vendor with broad OAuth access to many customers, replay tokens, harvest credentials, repeat. **Every SaaS integration is a candidate.**

▸ **EDUCATION TECHNOLOGY WILL REMAIN A PRIORITY SECTOR**

Instructure two-incident sequence, PowerSchool, Udemy, Figure, and publicly-recruited targeting all point this direction. **The combination of large multi-tenant footprint, sensitive PII (including minors), constrained customer-side security maturity, and reputational pressure-to-pay produces an unusually attractive risk/reward ratio.**

▸ **THE SHINYSP1D3R RAAS WILL REACH PRODUCTION**

Operational deployment in mid-to-late 2026 is the working assumption. This will give SLH affiliates an encryption-based monetization path on top of the existing data-extortion model — expanding the threat from "data extortion only" to "data extortion + encryption + business disruption."

Plausible but uncertain

- *Whether SLH will fragment.* Trustwave SpiderLabs has noted the SLH brand may simply be appropriation of legacy group names by a smaller operator core; there is "no evidence" of a "formal, centralized organization." If the leadership cell is small, a successful arrest could meaningfully disrupt — but arrests so far have not.
- *Whether physical-harassment threats will escalate to incidents.* DoControl and others have documented threats — and in some reports, follow-through — against executives and families. The data is too thin to forecast scale.
- *Whether the group's claimed "retirement" announcements presage a meaningful pause.* History suggests not — such announcements (September 12, 2025) preceded the largest single-vendor breach of the year (Instructure, May 2026).

Implications for the higher-ed SaaS sector specifically

The risk to a higher-education multi-tenant SaaS vendor is now structurally elevated for the foreseeable future. Three dynamics are mutually reinforcing:

1. **The actor has explicitly named the sector.** Mandiant, BleepingComputer, Halcyon, and ReliaQuest all assess that ShinyHunters has been "systematically going after education technology companies" since at least late 2024.
2. **The market is concentrating.** A small number of vendors (PowerSchool in K-12 SIS, Instructure in higher-ed LMS, Ellucian and Anthology in higher-ed administrative systems, Workday in HR/finance, Salesforce in CRM) account for outsized market shares. Every breach at one of those vendors becomes a multi-thousand-institution event.
3. **Customer institutions cannot independently defend themselves against vendor breaches.** As Michael Klein, formerly of the U.S. Department of Education, put it in the PowerSchool context: "There was literally nothing districts could have done to prevent the data breach." The defensive burden falls on the vendor.

The "when, not if" framing

For any organization fitting the higher-ed SaaS profile, treating a ShinyHunters-style attempt as a "when, not if" scenario is no longer a rhetorical flourish — it is the operational baseline. ShinyHunters publicly recruits insiders by name of industry vertical. They publicly catalog targets on Telegram. They retain stolen credentials for years. They operate continuously across arrest cycles. They have explicitly stated their preference for multi-tenant SaaS targets.

▸ THE SEVEN DECISIONS THAT FOLLOW

- **Identity is the perimeter.** Spend as if it were.
- **OAuth-connected apps are credentials.** Treat them as such.
- **Help desk is a target.** Train accordingly.
- **Customers are part of your attack surface.** Help them defend themselves; require them to.
- **Logs in your SIEM**, not in the SaaS vendor's default retention. Always.
- **Negotiation posture is a board decision**, made before the breach. Not after.
- **Communications posture is a CEO decision**, made before the breach. Not after.

Final assessment

The ShinyHunters criminal collective, operating now within the Scattered LAPSUS$ Hunters alliance, is the single most consequential brand in English-speaking financial cybercrime as of mid-2026. Their tradecraft is unsophisticated by elite-APT standards. **What makes them dangerous is the combination of disciplined targeting, opportunistic credential harvesting, fluent social engineering, an open recruitment pipeline, and a public-extortion playbook calibrated to extract maximum settlement leverage from victims who cannot tolerate disclosure.**

For a higher-education SaaS vendor, the analytically honest assessment is that there is no defensive posture that reduces the risk of being *targeted* to zero. There is, however, a defensive posture that materially reduces the probability of successful intrusion and that materially limits the blast radius and the business impact if intrusion occurs. That posture is documented in Sections 6 and 7. The work of implementing it — and rehearsing the decisions that follow from it — is the work that distinguishes vendors who survive a ShinyHunters incident from vendors who do not.

Appendix A · Source attribution and confidence levels

This report distinguishes throughout between three confidence levels.

Confirmed attribution / public record

Sourced to primary documents: DOJ unsealed indictments and press releases (Raoult, Lane, Moucka, Binns, West, Stokes), FBI FLASH alerts (FLASH-20250912-001), CISA Joint CSA AA23-320A and its July 29, 2025 update, Mandiant / Google Threat Intelligence Group technical reports, and the public statements of named victim companies (Salesforce, Salesloft, Snowflake, Instructure, PowerSchool, AT&T, Workday, Allianz Life, Google, Cisco, and others).

Suspected attribution / analyst assessment

Sourced to reputable security vendors and journalism with named analysts and consistent corroboration: Sophos Counter Threat Unit, Palo Alto Unit 42, ReliaQuest, Trustwave SpiderLabs, EclecticIQ, SOCRadar, Flare, Obsidian Security, Truesec, ZeroFox, BleepingComputer, The Record / Recorded Future News, TechCrunch, Wired, CyberScoop, Dark Reading, CSO Online, K-12 Dive, Fortune. Where these sources disagree (e.g., on whether ShinyHunters and Scattered Spider should be treated as a single entity), the disagreement is preserved in the text.

Threat-actor claims and unverified reporting

Including the claimed scale of the Instructure incident (275 million users / 8,809 institutions), the European Commission claim, the SoundCloud claim, the Pornhub / Mixpanel claim, the Medtronic claim, and the October 19, 2025 "Sevy" claim of Shiny's arrest. These are reported as claims, not as facts.

Appendix B · Glossary

AA23-320A	CISA Joint Cybersecurity Advisory on Scattered Spider, originally November 2023, updated July 29, 2025.
AiTM	Adversary-in-the-Middle phishing technique that proxies legitimate authentication flows.
BL2C	Brigade de lutte contre la cybercriminalité, the cybercrime unit of the Paris Police Prefecture.
DLS	Data Leak Site, typically operated on Tor by extortion groups.
FERPA	Family Educational Rights and Privacy Act (20 U.S.C. § 1232g).
FLASH	FBI's category of advisories distributed via the Internet Crime Complaint Center (IC3).
GLBA	Gramm-Leach-Bliley Act and its Safeguards Rule, applicable to financial-aid data.
GTIG	Google Threat Intelligence Group (incorporating Mandiant).
OAuth	Open Authorization framework used for delegated third-party application access.
RaaS	Ransomware-as-a-Service.
SLH / SLSH	Scattered LAPSUS$ Hunters / Scattered Lapsus$ Shiny Hunters — the combined alliance brand.
SOQL	Salesforce Object Query Language.
The Com	A loose, primarily English-speaking online cybercrime ecosystem, also called "The Community."
UNCxxxx	Mandiant's "uncategorized" threat-cluster tracking. UNC5537, UNC6040, UNC6240, UNC6395, UNC6661, UNC6671 are all relevant to the ShinyHunters brand.

Appendix C · Recommended reading

The single most-valuable primary documents for verifying or extending this report:

- Google Cloud blog, *"UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion"* (June 2024)
- Google Cloud blog, *"The Cost of a Call: From Voice Phishing to Data Extortion"* (2025)
- Google Cloud blog, *"Widespread Data Theft Targets Salesforce Instances via Salesloft Drift"* (August 2025)
- Google Cloud blog, *"Tracking the Expansion of ShinyHunters-Branded SaaS Data Theft"* (January 2026)
- FBI IC3, FLASH-20250912-001, *"Cyber Criminal Groups UNC6040 and UNC6395 Compromising Salesforce Instances for Data Theft and Extortion"*
- CISA Joint Cybersecurity Advisory AA23-320A, *"Scattered Spider"* (November 2023, updated July 2025)

- Sophos Counter Threat Unit, *"Taking the shine off BreachForums"* (June 2025)
- Palo Alto Unit 42, *"Bling Libra's Tactical Evolution"* and *"The Golden Scale"* (2025)
- Trustwave SpiderLabs / The Hacker News, *"A Cybercrime Merger Like No Other"* (November 2025)
- BleepingComputer, *"Meet ShinySp1d3r: New Ransomware-as-a-Service created by ShinyHunters"* (November 2025)
- U.S. DOJ (W.D. Wash. and D. Mass.), Raoult and Lane indictment / sentencing materials
- ReliaQuest, *"ShinyHunters Targets Salesforce Amid Clues of Scattered Spider Collaboration"* (2025)
- Resecurity, *"Trinity of Chaos: The LAPSUS$, ShinyHunters, and Scattered Spider Alliance"* (2025)

Caveats and limitations

- **Knowledge cutoff is May 12, 2026.** Given the operational tempo of ShinyHunters / SLH, the landscape is likely to have evolved by any reading more than several weeks after this date.
- **Attribution in the ShinyHunters / Scattered Spider / LAPSUS$ ecosystem is genuinely contested.** Researchers disagree on whether to treat these as separate, partially merged, or unified. This report follows Mandiant's UNC-cluster discipline while acknowledging the alternative view. Where the text speaks of "ShinyHunters" as an actor, the reader should understand this as shorthand for "the brand and the operators currently aligned under it."
- **Some prominent claims rest on threat-actor statements only** — most notably the Instructure 275-million-user / 8,809-institution claim has not been corroborated in Instructure's own statements.
- **Forecasts are forecasts.** Section 9 is explicit about the distinction between high-confidence and plausible-but-uncertain projections.
- **No specific architectural assumptions have been made about any particular vendor.** The threat-model and recommendations sections deliberately address the generic higher-education multi-tenant SaaS vendor.
- **This report is not legal advice.** FERPA, GLBA, state breach-notification, U.K. GDPR, Kuwait CITRA, and Qatar PDPPL obligations should be reviewed with qualified counsel before any incident-response decisions are taken.

— END OF BRIEFING —

Published by The Crosswalk · thecrosswalk.news · May 12, 2026